NOTE ON SCHLÄFLI'S ELLIPTIC MODULAR EQUATIONS.

By Arthur Berry.

In a former paper in this journal* I proved some properties of the elliptic modular equations substantially in the form commonly known as Schläfli's equations. I worked with a modular function $x(\tau) = 2^{-1/6}\chi(\tau)$, where χ is Hermite's function† and showed that, for transformations of prime order n (> 3), (1) when n is of the form $4p - 1$, corresponding to $\tau = i$, $x = 2^{-1/4}$ the roots of the modular equations are equal in pairs and branched, each pair corresponding to a branch point of order 1 on the corresponding Riemann surface and that (2) when n is of form $4p + 1$, there are $n - 1$ roots equal in pairs and branched, and two isolated roots. I showed further that the two isolated roots are always of the form $\epsilon^\lambda x(i)$ (λ an integer, $\epsilon = e^{2i\pi/24}$), and that for $n = 8p - 3$, the two values of ϵ^λ are $\pm i$ ($\lambda = \pm 6$ $mod.$ 24), while for $n = 8p + 1$ both values are $- 1$, or both values 1, but was unable to give any simple criterion distinguishing these last two cases.

The object of this note is to establish these results as to the isolated roots in a somewhat simpler way, avoiding the rather troublesome quadratic transformation used before, and to distinguish between the last two cases.

It is known that for a modular substitution $\{(c + d\tau)/(a + b\tau), \tau\}$ of Hermite's first type (a, d odd, b, c even)

$$x\{(c + d\tau)/(a + b\tau)\} = \epsilon^\lambda x(\tau),$$

where $\lambda = \frac{1}{2}(b - c)(bcd - a)$;‡ a similar equation holds for substitutions of the second type, but as these can be derived from those of the first type by applying the substitution $T(T\tau = - 1/\tau)$ and we are only concerned with $\tau = i$, so that $T\tau = \tau$, it is enough to consider substitutions of the first type. Hence in order to prove that $x\{(48r + i)/n\} = \epsilon^\lambda x(i)$, it is enough to prove that it is possible to find integers a, b, c, d, where a, d are odd, b, c even and $ad - bc = 1$, and an integer r such that

$$(48r + i)/n = (c + di)/(a + bi). \tag{1}$$

If n is a prime number of the form $4p + 1$, it is a well known result that

---

* On Elliptic Modular Equations for Transformations of Orders 29, 31, 37; Vol. XXX, pp. 156–169.

† Sur la résolution de l'équation du quatrième degré; *Comptes Rendus*, Vol. 46 (1858), *Oeuvres*, Vol. II, p. 28.

‡ Tannery and Molk, *Fonctions Elliptiques*, Vol. II, Table XLVI.

we can choose a and b (a odd, b even) so that $a^2 + b^2 = n$.* With this choice of a and b (1) is equivalent to

$$ac + bd = 48r, \qquad (2)$$

$$ad - bc = 1. \qquad (3)$$

We can now choose c, d to satisfy (3) and can further arrange so that c is even d odd; if c', d' is one such solution, the general solution is $c = c' + 2ka$, $d = d' + 2kb$ (k integral), and (2) can be satisfied, if

$$2k(a^2 + b^2) + ac' + bd' \equiv 0, \quad mod\ 48,$$
or
$$kn \equiv -\tfrac{1}{2}(ac' + bd'), \quad mod\ 24;$$

since n is prime and $ac' + bd'$ is even, this congruence can be satisfied; a, b, c, d are now found, and r is given by (2).

It remains to determine the integer λ (*mod*. 24), which depends on the congruences *mod*. 3 and *mod*. 16, satisfied by a, b, c, d.

From (2) and (3), it follows at once that if any one of a, b, c, $d \equiv 0$, *mod*. 3, then either a and d or b and c satisfy this congruence and therefore also $\lambda \equiv 0$, *mod*. 3; if no one of a, b, c, $d \equiv 0$, then from (3) $ad \equiv -1$, $bc \equiv 1$, whence $b - c \equiv 0$, so that again $\lambda \equiv 0$. Thus in all cases $\lambda \equiv 0$, *mod*. 3.

The congruences *mod*. 16 are rather more troublesome. From (2) it follows at once that if $b = 2^k \times$ (odd integer), $c = 2^{k'} \times$ (odd integer), then $k' = k$, for $k = 1, 2, 3$, and $k' \geq 4$ for $k \geq 4$; hence for $k \geq 2$ (which is the same condition as $b \equiv 0$, *mod*. 8) $b - c \equiv 0$ *mod*. 16 and $\lambda \equiv 0$, *mod*. 8; if $k = 1$ or 2, $ad = bc + 1 \equiv 1$, *mod*. 4 and $a \equiv d \equiv \pm 1$, *mod*. 4, so that $a + d \equiv 2$, *mod*. 4. We now have $a(b - c) = (a + d)b - (ac + bd) \equiv (a + d)b$, *mod*. 16, by (2), whence $b - c = 2^{k+1} \times$ (odd integer), so that for $k = 1$, $b - c \equiv \pm 4$, *mod*. 16, $\lambda \equiv \pm 2$, *mod*. 8, and for $k = 2$, $b - c \equiv 8$, *mod*. 16, $\lambda \equiv 4$, *mod*. 8. As we have seen that $\lambda \equiv 0$, *mod*. 3 it follows that $\lambda = \pm 6, 12, 0$, *mod*. 24 and $\epsilon^\lambda = \pm i, -1, 1$ according as $k = 1$, $k = 2$, $k > 2$. The condition $k = 1$ (or $b \equiv 2$, *mod*. 4) can be replaced by the simpler condition $n \equiv -3$, *mod*. 8, for a^2 being the square of an odd number is necessarily of the form $8p + 1$, so that $b^2 = n - a^2 \equiv n - 1$ *mod*. 8, and then $b \equiv 2$, *mod*. 4 or $b \equiv 0$ *mod*. 4 according as $n \equiv -3, 1$, *mod*. 8.

The discrimination between the cases $k = 2$, $k > 2$ (or $b \equiv 4$, $b \equiv 0$, *mod*. 8), does not appear possible by means of any linear congruence for n but requires the actual expression of n ($n = 8p + 1$) in the form $a^2 + b^2$ or some equivalent process in the arithmetical theory of quadratic forms.

---

* Mathews, *Theory of Numbers*, § 91.

By the proof already given if one isolated root is known the other is its conjugate imaginary, so that if one is $\pm ix(i)$, $= \pm i2^{-1/4}$ the other is $\mp ix(i)$, and if one is $\pm x(i)$ the other is equal to it.

Thus we have the final result:

If $n \equiv -1\ mod.\ 4$, all the roots correspond to branch points; if $n \equiv -3$, *mod.* 8, there are two isolated roots $\pm i2^{-1/4}$; if $n \equiv 1$, *mod.* 8, there are two isolated roots both $-2^{-1/4}$ or both $2^{1/4}$ according as, when n is expressed in the form $a^2 + b^2$ (a odd, b even), $b \equiv 4$ or $b \equiv 0$, *mod.* 8.

I take the opportunity of correcting some errata in my former paper:

P. 158, line 11, *for* mod. 48 *read* mod. 24.

P. 165, line 18, *for* $x\{(-1 + i\sqrt{27})/31\}$ *read* $x\{(-2 + i\sqrt{27})/31\}$.

P. 165, line 23, *for* 24 *read* 2^4.

P. 165, lines 23, 26, *for* $\sqrt{19}$ *read* $\sqrt{15}$.